IN THE CLAIMS:

Please amend claims 1-3, 5, 6, 8, 9, 22, 28, 30, 34, 35, 48, and 49; cancel claims 10-21 without prejudice or disclaimer; and add new claims 50 and 51 as follows.

1. (Currently Amended) An apparatus, comprising:

a proxy configured to receive a request for network services by at least one remote network device and to perform a security integrity scanning operation on the requesting remote network device, wherein the security scanning operation is performed ~~at least~~ before and after the remote network device signs on to the proxy; and

an authorization processor and access rules controller configured to determine if the remote network device is authorized to access the requested network services based on the results of the security scanning operation.

2. (Currently Amended) The apparatus as recited in claim 1, wherein the proxy ~~makes~~ is configured to make integrity security decisions regarding access to network services by a remote network device on a request-by-request basis.

3. (Currently Amended) The apparatus as recited in claim 1, wherein the access rules controller ~~includes~~ comprises a plurality of variables used to generate a set of security properties for each remote network device.

4. (Original) The apparatus as recited in claim 3, wherein the set of security properties may be different for each remote network device that accesses and requests service through the network.

5. (Currently Amended) The apparatus as recited in claim 1, wherein the proxy ~~uses~~ is configured to use at least one script to select of the type of scanning operations to be performed for each remote network device accessing the network.

6. (Currently Amended) The apparatus as recited in claim 5, wherein the proxy ~~uses~~ is configured to use a Java applet to execute the desired script on the remote network device.

7. (Previously Presented) The apparatus as recited in claim 6, wherein a signed applet executing the script, is allowed to access the remote network device for the purposes of executing programs as well as to search and read specific data files that reside on the remote network device.

8. (Currently Amended) The apparatus as recited in claim 1, wherein the authorization processor ~~refers~~ is configured to refer to a series of variable values in the access rules controller to determine if a remote network device is authorized to access the requested network service.

9. (Currently Amended) A system, comprising:

at least one remote network device configured to access a network via a network connection to make a request for one or more network resident services;

a gateway configured to receive the request for services and perform a security integrity scanning operation on the remote network device prior to allowing access to the requested network services, wherein the security scanning operation is performed ~~at least~~ before and after the remote network device signs on to the gateway;

an authentication server configured to verify user authentication credentials of users of remote network that access the network; and

at least one network server configured to provide requested network services to at least one remote network accessing the network through the gateway.

10-21. (Cancelled)

22. (Currently Amended) A method, comprising:

performing scanning process and reporting result used in scanning script, ~~including~~ comprising at least one variable defined to be used as a vehicle to convey results of a scanning process;

performing at least one scanning operation on the remote network device to verify a security integrity of the remote device, wherein the scanning operation is performed ~~at~~

~~least~~ before and after the remote device signs on to a gateway device which is configured to perform the ~~at least one~~ scanning operation; and

providing the results of the scanning operation for purposes of determining whether or not the remote network device is authorized to access the requested network services.

23. (Original) The method as recited in claim 22 wherein, the making of security decisions with regard to a request for network services by a remote network device is done on a per-request basis.

24. (Previously Presented) The method as recited in claim 22 wherein, an array of variables is used to generate a set of security properties for each remote network device.

25. (Original) The method as recited in claim 24, wherein the set of security properties may be different for each remote network device that accesses and requests service through the network.

26. (Previously Presented) The method as recited in claim 22, further comprising:

selecting at least one script for the type of scanning operation to be performed for each remote network device that accesses the network.

27. (Previously Presented) The method as recited in claim 26, further comprising:

executing the desired script on the remote network device by using a signed Java applet.

28. (Currently Amended) The method as recited in claim ~~16~~27, further comprising:

using a signed applet for executing the script to access the remote network device for the purposes of executing programs, searching, and reading specific data files that reside on the remote network device.

29. (Previously Presented) The method as recited in claim 22, further comprising:

assigning a values to a set of variables in the verification software resulting from the scanning process of the remote network device.

30. (Currently Amended) The method as recited in claim 22, further comprising ~~using~~:

using secure socket layer to protect the data communicated between the remote device and the gateway.

31. (Previously Presented) The method as recited in claim 29, wherein referencing an assigned series of variable values in the access control rules determines if a remote network device is authorized to access the requested network service.

32. (Previously Presented) The method as recited in claim 22, further comprising:

making authorization decisions based in part on results returned by the scanning process.

33. (Previously Presented) The method as recited in claim 22, further comprising:

transmitting and receiving data, information and applications content between a remote device and the gateway comprises global system for mobile communications, general packet radio service, wireless application protocol, enhanced data for global system for mobile communications evolution, or universal mobile telecommunication system .

34. (Currently Amended) The method as recited in claim 22, wherein the remote network device is a public kiosk, personal computer, cellular telephone, satellite telephone, personal assistant or ~~BLUETOOTH~~ Bluetooth device.

35. (Currently Amended) A method, comprising:

defining at least one access control policy for accessing network services wherein the access control policy depends, at least in part, on the results of an integrity scan performed on a remote network device;

specifying what scan scripts are to be used under what conditions to the remote network device;

receiving at least one result of an integrity scan from the remote network device at a gateway device, wherein the integrity scan is performed ~~at least~~ before and after the remote device signs on to the gateway device; and

regulating access by the remote network device to network services via the gateway device based, at least in part, on the results of the integrity scan.

36. (Previously Presented) The method as recited in claim 35, further comprising:

making access control decisions with regard to a remote network device on a per-service basis.

37. (Previously Presented) The method as recited in claim 35, further comprising:

using at least one defined variable in each access control policy.

38. (Previously Presented) The method as recited in claim 35, further comprising:

sending the results of the integrity scan to the gateway in the form of an assigned value for the defined variable.

39. (Previously Presented) The method as recited in claim 35 further comprising:

using a script to specify the integrity scan operations that will be performed on the remote network device.

40. (Previously Presented) The method as recited in claim 35, further comprising:

using a signed Java applet as verification software to be downloaded to the remote network device.

41. (Previously Presented) The method as recited in claim 39, further comprising:

using a signed applet executing the script to access the remote network device for executing programs, searching, and reading specific data files that reside on the remote network device.

42. (Original) The method of claim 35, wherein a plurality of variables is used to determine the access control policy for each remote network device accessing the network.

43. (Original) The method as recited in claim 42, wherein the access control policy for each remote network device is different.

44. (Previously Presented) The method as recited in claim 38, wherein referencing to an assigned series of variable values in the access control rules determines if a remote network device is authorized to access the requested network service.

45. (Previously Presented) The method as recited in claim 35, further comprising:

using secure socket layer to protect data communicated between the remote device and the gateway.

46. (Previously Presented) The method as recited in claim 35, further comprising:

making authorization decisions based in part on results returned by the scanning process.

47. (Previously Presented) The method as recited in claim 35, further comprising:

transmitting and receiving data, information and applications content between a remote device and the gateway using either global system for mobile communications, general packet radio service, wireless application protocol, enhanced data for global system for communications evolution, universal mobile telecommunication system or other similar wireless network protocol.

48. (Currently Amended) The method as recited in claim 35, wherein the remote network device is a public kiosk, personal computer, cellular telephone, satellite telephone, personal assistant or ~~BLUETOOTH~~ Bluetooth device.

49. (Currently Amended) An apparatus, comprising:

proxying means for receiving a request for network services by at least one remote network device and to perform a security integrity scanning operation on the requesting

remote network device, wherein the security scanning operation is performed ~~at least~~ before and after the remote network device signs on to the proxy; and

authorization processing means and access rules controlling means for determining if the remote network device is authorized to access the requested network services based on the results of the security scanning operation.

50. (New) A computer program, embodied on a computer-readable medium, configured to control a processor to implement a method, the method comprising:

performing scanning process and reporting result used in scanning script, including at least one variable defined to be used as a vehicle to convey results of a scanning process;

performing at least one scanning operation on the remote network device to verify a security integrity of the remote device, wherein the scanning operation is performed before and after the remote device signs on to a gateway device which is configured to perform the scanning operation; and

providing the results of the scanning operation for purposes of determining whether or not the remote network.

51. (New) A computer program, embodied on a computer-readable medium, configured to control a processor to implement a method, the method comprising:

defining at least one access control policy for accessing network services wherein the access control policy depends, at least in part, on the results of an integrity scan performed on a remote network device;

specifying what scan scripts are to be used under what conditions to the remote network device;

receiving at least one result of an integrity scan from the remote network device at a gateway device, wherein the integrity scan is performed before and after the remote device signs on to the gateway device; and

regulating access by the remote network device to network services via the gateway device based, at least in part, on the results of the integrity scan.